International Journal of Advances in Computer Science & Its Applications
Volume 6 : Issue 2 [ISSN 2250-3765]
Publication Date : 31 August, 2016

Electronic techniques for countering social-engineering cyber crimes

Leonard J. Mselle

***Abstract*—In this paper the basic definitions of the prominent social engineering techniques used to carry out cyber crimes (specifically money theft) are broadened. The prominent social-engineering physical and psychic-logical doors of attack are expounded. A scheme for electronic remedies (automatons) is proposed. Algebraic primitives for lemmas/corollaries for automatons for countering social engineering crimes are proposed. Alternative architectures for cyber-crime detecting automatons (CC-DAs) are proposed and discussed.**

***Keywords*—cyber security, social engineering, lemma, automatons.**

I. Introduction

Money or information theft trough electronic means is now a common phenomenon due to proliferation of electronic services ranging from; banking, health, educational, entertainment, etc. Most of illicit money acquisition through electronic means in Tanzania is done through social engineering techniques [1]. However, in the literature, social engineering through mobile phones is completely neglected. There is a need to bridge this gap by expanding the definitions of social engineering techniques with mobile phones in mind.

A. *Expansion of basic definitions of major social engineering techniques*

Havey [2] defines social engineering as the use of non-technical means to gain unauthorized access to information or systems. Instead of using vulnerability and exploit scripts, social engineering usually refers to the process of convincing a person to reveal information (such as a password) that enables the hacker to gain access to a system or network. This definition is narrow since it precludes the use of mobile phones to execute cyber crimes. In a typical case, mobile phones constitute the most frequently means used to realize money theft than computers or other communication devices or means.

Through telephone calls/message, criminals exploit non visibility and distance separation in combination with a class of glib conversations to convince victims to send them money or valuable information through electronic transfers. The money or information may be sent to an account in the bank or to the mobile phone of the criminal's choice/suggestion. Phishing is among the most popular subclasses of social engineering that are common in Tanzania.

B. *Phishing*

Scambray and Shema [3] describe phishing as a social engineering technique used to infect the system(s) with malicious codes or glib information used to obtain personal or sensitive information. It involves the mass distribution of fraudulent electronic messages with return addresses, links and branding which appear to come from legitimate organizations such as banks insurance agencies, retailers or credit card companies. They normally appear as important notices, urgent updates or alerts with deceptive subject line to attract the recipient to believe that the electronic message has come from a trusted source. This definition again, precludes mobile phone phishing which is typical in Tanzanian context. Applying this technique, a criminal sends a message or calls the victim, such that the criminal pretends to be a legal entity such as; electricity utility company or masquerades as a person who is known to the victim. In the discourse, the criminal ends up suggesting to the victim to pay a certain amount of bill/money to a certain account or to a mobile phone number which the criminal purports to belong to the utility company or to a genuine recipient, while in reality, the account that belongs to the criminal. Along with phishing there is spoofing.

C. *Spoofing*

Spoofing is another popular social engineering technique which covers a broad category of threats. In general terms, a spoof entails falsifying one's identity or masquerading as a certain individual or entity to gain access to a system or network or to gain information in unauthorized way. There are various kinds of spoofs, including, among many others, IP address spoofing, session hijacking, domain name service (DNS) spoofing, sequence number spoofing, and replay attacks [3 & 4]. Again this definition precludes mobile phone spoofing which has been used to rob most of mobile money service providers and

Leonard J. Mselle
The University of Dodoma
Tanzania

users (e-money agents, such as tigoPesa, M-Pesa, Airtel Money, etc). Often, this technique involves insider trading on the part of the carrier company. In this regard, the victim's mobile line is temporarily hijacked by criminals who identify themselves as the genuine owner of the line. A communication that is used to order a certain transfer of money to the number dictated by the criminal is performed. After the transaction is performed the line is restored back to its legitimate owner.

Normally, individuals and even corporations find it hard to report attacks that stem from social engineering for fear of affecting customer's confidence and hurting personal esteem [2 & 3]. Where complaints are reported, specifically to the police, these reports are made after the event which makes arraigning the criminals difficult if not impossible. Electronic social engineering has various doors of attack that can be categorized in physical and psychic-sociological.

II. The prominent social engineering physical doors of attack

Among the common physical doors through which social engineering crimes are carried out include; mobile phones, bank accounts and online money facilities (SIM banking which provides online ability for the criminals to check the bank balance, facilitating criminals to use bank accounts to become thieves/predators). Victims are all customers gullible enough to accept the baits.

Mobile telephones and electronic money facilities allow for a straight-forward money exchange whereby the cheated victim is made to transfer money to a telephone number or an account owned by the criminal. Victims are all unsuspecting customers who may happen to believe and participate in a shoddy scheme which apparently is provides the victim with a possibility of making some easy money fast.

Telephone money transfer facilities combined with phishing and spoofing are part of the doors cyber crimes. In this case, sometimes by assistance from insider trading from the carrier company the telephone line of the electronic money agent such as Mpesa, Tigo pesa and Airtel money is spoofed (temporarily hijacked) by a cyber criminal. The criminal, masquerading as the owner (phishing) of the business, issues an order to the subordinate to send money to a given telephone number which happens to belong to the criminal. After the unsuspecting subordinate effects the transaction the spoofed number is restored to its original owner. These physical doors are used for robbery in combination with psychic logical doors.

A. *The prominent social engineering psychic-logical doors of attack*

The most prominent social-psychic logical cyber crime doors of attack include; impersonation by the criminal, human greed, natural inclination to get rich quick, natural attraction to help, ignorance on the part of victims and unpreparedness/lack of proper coordination among law enforces and consumer protection agencies.

One or a combination of the various of psychic-logical doors with one or various of the physical doors makes it possible for a cyber crime to be executed. So far in Tanzania, money theft incidents through cyber space have been in ascendance. Dodoma region police has had more than 2000 reported cases in a period of three years. The situation is not predicted to improve any time soon. Inadequate posture by the agencies to combat cyber crime is the main source of the bleak future. Incidents are reported posthumously, later the police attempts, unsuccessfully, to pursue the issue. The police force is complaining that cooperation from carrier companies is not forthcoming. In addition, the police force is underequipped. There is no a commonly agreed flow chart(s) between regulators, police force and carriers for handling the incident. In the meantime, cyber criminals continue to scam users unhindered and are not going to stop anytime soon. They have been benefiting from lack of scrutiny, and effective means to arraign them. This is a situation that necessitates electronic intervention. There is no evidence of existence of a general framework for developing automatons (languages) special for detecting social engineering speech and in turn alert the victim.

III. Problem statement

So far, education campaigns and corporate policies have been the basic means used to combat cyber social engineering. In most cases, criminals have found alternative means to circumvent these counter measures. The psychic logical doors of attack in combination with the physical doors have proved more vulnerable due to the fact that arraigning these criminals or stopping them will require coordination from users, police force, carriers and regulators and banks which is next to impossible. There exists no evidence of a complete body of algebraic formulae and derived automatons for combating social engineering. In Tanzania for example there is no single electronic remedy that has been proposed to respond to any of the classes of social engineering technique. It is predicted in this paper that electronic remedies (automatons) based on string property detection can be designed and be embedded in telephones to alert customers and other responsible organs in case of social engineering conversation/attempt.

IV. Proposed electronic remedies (automatons)

It is postulated in this paper thus;

1. Electronic social engineering techniques used to execute cyber theft can be detected electronically through electronic automatons.
2. These social engineering techniques are context sensitive and therefore the proposed electronic automatons will be context-sensitive turing machines whose patterns recognition algorithms can be expressed by context-based algebraic expressions.
3. Such automatons can be embedded in telephone systems connecting the National CERT, mobile telephone carriers, banks and the Police Force (jointly or separately) to; stop cyber crime, issue

security warnings, notify users of possible attacks, block the account or communication connection, redirect the transaction, delay the transaction as one of options to mitigate or stop possible cyber crime, while facilitating the arrangement of the criminals if the victims choose so.

V. Proposed lemma for automatons for countering social engineering mobile money crime

In order to design and develop automatons for detecting and countering social engineering (mobile telephone phishing and spoofing) the first step is to propose the basic vocabulary, and then proceed to evolve necessary tautologies which will be used to define lemma/corollary for a class of automatons that deals with social engineering.

A. *The basic vocabulary*

The basic vocabulary for a lemma, automaton and function derivation is adopted from [5] as follows;

1. There is set ***W*** of internal states
2. There is set ***Z*** of possible input vocabulary/pattern
3. There is set ***Y*** output signals
4. A specification by function $\delta: W \times Z \rightarrow W$ (1) of how the current state and the current input determines the next state.

B. *Basic 7 tautologies for a lemma, S, fitting a conversation leading to a cyber theft*

A toxic *conversation lemma*, ***S,*** is proposed, such that;

$\boldsymbol{A \Longrightarrow B}$ (2).

is a ***toxic conversation*** with initial input (***W***) that satisfies the following ***necessary conditions***;

1. A mobile phone conversation, $\boldsymbol{A \Longrightarrow B}$ is initiated between ***A (Pray)*** and ***B (Predator)*** such that;
   $\boldsymbol{A \Longrightarrow B}$ (X) was initiated by ***B*** (3).
2. Over the time, ***(t)*** during the conversation **A**$\Longrightarrow$**B**, B proposes to A ***a money-making venture*** $V \varepsilon Z$ such that ***A will earn*** ∑, amount of money as a result of B’s middleman’s-ship/transfer (state ***w0 ε W***) (4).
3. Over time ***(t+n)*** > ***t*** of the conversation $\boldsymbol{A \Longrightarrow B}$, B proposes that ***A pays*** a certain amount of ***money*** *M,* such that;
   M ***which is always < ∑, covers some preliminary expenses*** of the venture **V ε *X*** (next state ***w1ε W***) (5).
4. Further, A proposes that the amount, *M* ***must be sent immediately*** through either a ***Bank account*** or ***a telephone number proposed by A*** (next state ***w2 ε W***) (6).
5. ***venture*** $V \varepsilon Z$ requires some secrecy and money exchange, specifically the amount ***Y must be sent immediately*** before anything else is done (next state ***w3 ε W***) (7).
6. If conditions 1 through 5 are satisfied then ***W*** $\Longrightarrow$ ***W1 (is necessarily a toxic conversation, W1***) that requires/triggers an output/action (***Y***) from the automaton (8).
7. ***Y*** (Action/output signal by automaton to either; ***warn the pray/cut conversation/alert the user/police/CERT/Bank***).

Consequently, a ***generic social engineering detector/stopper automaton***, ***CC-DA*** is defined thus;

CC-DA (finite) is a quintuple;

$S = \{W, Z, Y, (finite), \delta, \lambda\}$ (9) where:

1. ***W, Z*** and ***Y*** are sets of states, inputs and outputs respectively.
2. $\boldsymbol{\delta: W \times Z \rightarrow Z}$ and $\boldsymbol{\lambda: W \times Z \rightarrow Y}$ are functions called the next state and current output functions respectively (10).

VI. Alternative architectures of CC-DA

From the defined generic automaton, S= *{W, Z, Y, (finite), δ, λ}* various models according to the contexts can be designed and developed**.**

A. *CERT model architecture*

Under this architecture, CC-DA will detect the general call and speech-patterns such that the basic characteristics satisfy the set of the patterns as depicted in Fig. 1.

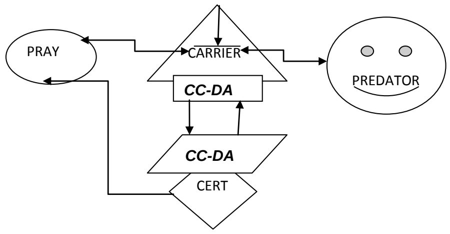

Fig. 1. The CERT model automaton architecture

Description of the mechanisms of the CERT Model

The PREDATOR will always initiate the conversation through CARRIER. The DETECTOR senses that the conversation is turning TOXIC/cyber crime likely to be committed. The detector triggers the LISTENER which is under CERT. The LISTERNAR determines that the PRAY is about to be victimized/cybercrime definitely being committed. It advises CERT to take protective action which will be to WARN the PRAY or cut the conversation or arrange for arraignment of the PREDATOR by help of the police.

B. The Police model architecture

Under police model architecture, CC-DA will detect the general call and speech-patterns such that the basic characteristics satisfy the set of the patterns as depicted in Fig. 2.

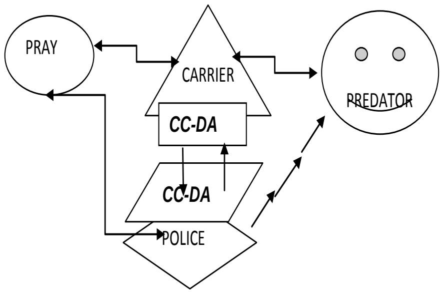

Fig. 2. The police model automaton architecture

Description of the mechanisms of the CERT Model

Under this model, the PRAY/willing customers will voluntarily subscribe to the ***CC-DA***, the DETECTOR facility through CARRIER. The PREDATOR will initiate the conversation through CARRIER. When the DETECTOR senses that the conversation is turning TOXIC/cyber crime likely to be committed it will trigger the LISTENER which is under POLICE. The LISTERNER will determine if the PRAY is about to be victimized, that is, cybercrime is definitely going to be committed. The LISTERNER will advises the POLICE to take protective action, WARN the PRAY or cut the conversation. POLICE will initiate the move for arraignment of the PREDATOR.

C. The Banker's model Architecture

Under this architecture, CC-DA will detect the general call and speech-patterns such that the basic characteristics satisfy the set of the patterns as depicted in Fig. 3.

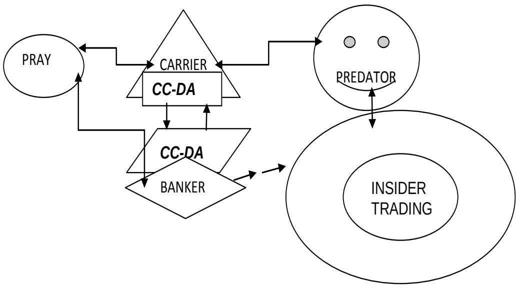

Fig. 3. The banker's model automaton architecture

Description of the basic mechanisms of the Bankers Model

Offline, there will be a routine check by ***CC-DA*** (DETECTOR) for possible predatory accounts by checking patterns that identify a possible toxic account. Upon detecting such accounts the automaton will trigger repossession/registration and tagging of accounts by fraud directorate.

An On line module will require customer's voluntary subscription. The PRAY/willing-customers will voluntarily subscribe to the DETECTOR facility through the bank. Live detection will occur when the PREDATOR initiates the conversation through CARRIER. The DETECTOR will sense that the conversation is turning TOXIC/cyber crime likely to be committed. The sensor will trigger the LISTENER which is under BANK FRAUD UNIT. The LISTERNAR will determine that the PRAY is about to be victimized/cybercrime definitely going to be committed. The LISTERNAR advises the BANK FRAUD UNIT to take protective action, WARN the PRAY or cut the conversation. It will initiate the move to arrange for arraignment of the PREDATOR. It will proceed to detect whether there is insider trading case behavior and notify the police.

D. The User-lone model architecture

Under this architecture, ***CC-DA*** will detect the general ***call and speech patterns*** such that the basic characteristics satisfy the set of the patterns as depicted in Fig. 4.

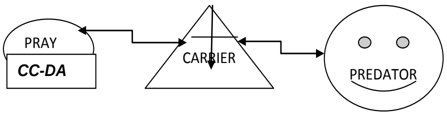

Fig 4. The user model automaton architecture

Description of the basic mechanisms of the User lone Model

The customer/user acquires and activates the automaton in his/her mobile phone. On-line detection will occur when the PREDATOR initiates the conversation through CARRIER. The DETECTOR will sense that the conversation is turning TOXIC/cyber crime likely to be committed. The detector will WARN the PRAY and cut the conversation.

VII. Recommendations

Carrier companies and banks will be the major losers if mobile cyber crime continues unabated. Unless these criminals are stopped, user will lose confidence in electronic money facilities and this line of business will be severally undermined. In Tanzania, social engineering cyber crime continues unabated. Those that will be able to secure their infrastructure against social engineering will benefit from improved customer confidence. Currently, there are no business concerns that are investing in research and development of indigenous cyber security tools which are context sensitive. If this trend continues, Tanzanian businesses will be forced to rely on foreign products and experts who will definitely be very expensive. Using universities to design, develop and test such tools is one of the most feasible alternatives.

References

[1] TCRA, "Tanzania's cyber security posture: End of Year I Report", 2014.

[2] S. Havey, "Crypto", Penguin Group, 2001.

[3] J. Scambray and M. Shema "Hacking Exposed Web Applications", McGraw-Hill, London, 2009.

[4] Schiller et al. "Botnets the killer web App," [http://www.Syngress.com]. 2008.

[5] L. Bobrowand and M. A. Arbib "Discrete Mathematics: Applied algebra for Computer and Information science", W. B. Saunders Co., Philadelphia,.1974.

About Author (s):

Prof. Leonard J. Mselle, is a senior lecturer at the Department of Computer Science of the University of Dodoma. Prof. Mselle is a renown world researcher in the areas of *computer programming*, *programming languages* and *cyber security*. He has published six books in the areas of computer programming and programming languages. Prof. Mselle is the inventor of **Memory Transfer Language** (MTL), an artificial language used for learning and teaching programming in both low and high level languages. Prof. Mselle has presented and published more than 27 scientific papers in various conferences and international journals.